WHAT IS CLAIMED IS:

1. A method for evaluating random numbers generated by a random number generator, the method comprising the steps of:

generating a continuous stream of random bits;

storing said generated random bits in a memory medium;

shifting said stored random sequences by a predetermined amount;

computing modified products of bit sequences between said stored random sequences and said shifted random sequences to determine an average correlation value; and,

determining whether said generated random numbers are sufficiently random by comparing said determined average correlation value to a predetermined acceptance range.

2. The method of claim 1, wherein the value of said modified products is one of -1's and +1's.

3. The method of claim 2, further comprising the step of determining that said generated random numbers are not sufficiently random when any of the average autocorrelation values does not fall within said predetermined acceptance range.

4. The method of claim 2, further comprising the step of notifying that said generated random sequences are not sufficiently random when any of the average autocorrelation values falls outside said predetermined acceptance range.

5. The method of claim 2, further comprising the step of generating a new set of random sequences when any of the average autocorrelation values falls outside said predetermined acceptance range.

6. The method of claim 1, further comprising the step of applying said dot products to a plurality of exponential averaging operations (A) each time a new bit is generated.

7. The method of claim 6, wherein said exponential averaging operations (A) are updated according to the following equation:

$A_{new} = \alpha \cdot A_{old} \pm 1,$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$).

8. The method of claim 6, further comprising the step of determining that said generated random numbers are not sufficiently random when the output of any of said exponential averaging operations (A) falls outside said predetermined acceptance range.

9. A method for evaluating the random numbers generated by a random number generator, the method comprising the steps of:

(a) generating and storing a stream of random bits using said random number generator;

(b) shifting said stored random sequences by a predetermined amount;

(c) computing modified products of bit sequences between said stored random numbers and said shifted random numbers;

(d) performing exponential averaging operations (A) on said modified products to obtain average autocorrelation values;

(e) comparing the average autocorrelation values to a predetermined acceptance range; and,

(f) determining that said generated random numbers are not sufficiently random when any of the average autocorrelation values falls outside said predetermined acceptance range.

10. The method of claim 9, further comprising the step of:

repeating said steps (a) - (e) until any of said computed exponential averaging operations (A) falls outside said predetermined acceptance range.

11. The method of claim 9, further comprising the step of notifying that non-random numbers are generated when said steps (a) - (e) are repeated more than a predetermined number of times.

12. The method of claim 9, further comprising the step of generating a new set of random numbers when said steps (a) - (e) are repeated more than a predetermined number of times.

13. The method of claim 9, further comprising the step of updating said exponential averaging operation (A) according to the following equation:

$A_{new} = \alpha \cdot A_{old} \pm 1,$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$).

14. An apparatus for evaluating the random numbers generated by a random number generator, comprising:

a random generator unit for generating random sequences comprising of binary bits;

a detector unit, coupled to the output of said random generator unit, for detecting whether said generated random sequences are sufficiently random; and,

a switching unit, coupled to the outputs said random generator and said detector unit, for disabling the flow of said generated random sequences for a subsequent application when said generated random sequences are determined to be insufficiently random,

wherein said generated random bits are stored and shifted by a predetermined amount to obtain modified products of bit sequences between said stored random sequences and said shifted random sequences, said modified products applied to exponential averaging operations (A) to determine an average autocorrelation value and wherein, if the output of any of said exponential averaging operations (A) falls outside a predetermined acceptance range, determining that said generated random sequences are insufficiently random.

15. The apparatus of claim 14, further comprising means for transmitting an alarm signal when any of the output of said exponential averaging operations (A) falls outside said predetermined acceptance range.

16. The apparatus of claim 14, wherein said exponential averaging operation (A) is performed according to the following equation:

$A_{new} = \alpha \cdot A_{old} \pm 1,$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$).

17. A machine-readable medium having stored thereon data representing sequences of instructions, and the sequences of instructions which, when executed by a processor, cause the processor to:

store a plurality of bits of externally generated random sequences of binary bits;

shift said stored random sequences by predetermined amounts;

compute a modified dot product of bit sequences between said stored random sequences and said shifted random sequences to determine an average autocorrelation value; and,

determine whether said generated random numbers are sufficiently random by comparing all said determined average autocorrelation values to a predetermined acceptance range.

18. The memory medium of claim 17, wherein said generated random numbers are determined to be insufficiently random when any of the average autocorrelation values falls outside said predetermined acceptance range.

19. The memory medium of claim 17, wherein said processor is further operative to generate a new set of random bits when any of the average autocorrelation values falls outside said predetermined acceptance range.

20. The memory medium of claim 17, wherein said processor is further operative to apply said modified product to an exponential averaging operation (A) each time a new bit is generated.

21. The memory medium of claim 21, wherein said exponential averaging operation (A) is computed according to the following equation:

$A_{new} = \alpha \cdot A_{old} \pm 1,$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$).